AMENDMENTS TO THE CLAIMS

Kindly amend claims 1, 17, 18, 26, 45, and 46 in accordance with the following:

1. (Currently amended) A method ~~Method~~ for documenting a transfer of authority of control for a container from a first entity of a transportation chain to a second entity of the transportation chain, the method comprising:

receiving in an electronic seal associated with the container ~~wherein the first entity transfers~~ an electronic container control certificate associated with a first entity, ~~to an electronic seal of the respective container, which~~ the electronic container control certificate comprises a cryptographic key associated to the second entity, and which container control certificate is digitally signed by the first ~~entity~~ entity; and

receiving in the electronic seal associated with the container, geographic location data from a location recording device associated with one of the first and second entities.

2. (Original) Method according to claim 1, comprising storing the container control certificate in a log of the electronic seal.

3. (Original) Method according to claim 1, comprising verifying the signed container control certificate by a corresponding function implemented in the electronic seal.

4. (Original) Method according to claim 3, comprising verifying the digital signature of the container control certificate by applying decrypt information stored in the log of the electronic seal and delivered to the log by a previous entity of the transportation chain.

5. (Original) Method according to claim 4, wherein the verification is considered to be failed if the signed container control certificate cannot be decrypted with the decrypt information stored in the log.

6. (Previously presented) Method according to claim 3, wherein a status of a container

lock is subject to the result of the signature verification process.

7. (Previously presented) Method according to claim 3, wherein the electronic seal issues a warning if the verification of the signature fails.

8. (Previously presented) Method according to claim 3, wherein the container control certificate is stored in the log if the verification succeeds.

9. (Previously presented) Method according to claim 1, wherein the cryptographic key associated to the second entity is used by the electronic seal for decrypting data expected to be received from the second entity.

10. (Previously presented) Method according to claim 1, wherein the electronic seal is designed for controlling a lock of the container.

11. (Previously presented) Method according to claim 1, wherein an asymmetric cryptographic key system is used for digitally signing the container control certificate.

12. (Original) Method according to claim 11, wherein a public--private key system is used for digitally signing the container control certificate.

13. (Original) Method according to claim 12, wherein the container control certificate is signed using a private key associated to the first entity.

14. (Previously presented) Method according to claim 4, wherein the container control certificate is signed using a private key associated to the first entity and the decrypt information stored in the log comprises a public key of the first entity.

15. (Previously presented) Method according to claim 1, wherein the first entity receives the cryptographic key associated to the second entity from a certificate authority.

16. (Previously presented) Method according to claim 1, wherein the container control certificate comprises identification data for the container.

17. (Cancelled) Method according to claim 1, wherein a location recording device associated to one of the entities transfers location data to the electronic seal.

18. (Currently amended) Method according to ~~claim 17~~ claim 1, wherein the location data is digitally signed by the associated entity.

19. (Previously presented) Method according to ~~claim 17~~ claim 1, wherein the signed location data is stored in a log of the electronic seal.

20. (Previously presented) Method according to ~~claim 17~~ claim 1, comprising verifying the signed location data by a corresponding function implemented in the electronic seal.

21. (Original) Method according to claim 20 comprising verifying the digital signature of the location data by applying decrypt information stored in the log of the electronic seal and delivered to the log by a previous entity of the transportation chain.

22. (Previously presented) Method according to claim 20, wherein the verification is considered to be failed, if the signed location data cannot be decrypted with decrypt information stored in the log.

23. (Previously presented) Method according to claim 20, wherein recording the location data in the log of the electronic seal is subject to a result of the signature verification process.

24. (Previously presented) Method according to claim 1, wherein the electronic seal transmits container identification information to a location recording device associated to one of the entities.

25. (Previously presented) Method according to claim 24, wherein the transmitted container identification information is digitally signed by a second entity.

26. (Cancelled)

27. (Original) Computing unit for communicating with an electronic seal of a container, the computing unit comprising

an interface for transferring data to the electronic seal, and

a control unit designed for

assembling an electronic container control certificate, the container control certificate comprising a cryptographic key associated to an entity different from the entity the computing unit is associated to,

digitally signing the container control certificate on behalf of the associated entity, and

submitting the digitally signed container control certificate to the interface.

28. (Original) Computing unit according to claim 27, comprising

an interface for communicating to a certificate authority;

the control unit being designed for requesting the cryptographic key associated to the different entity from the certificate authority.

29. (Original) Computing unit according to claim 18, comprising a log for storing a cryptographic key associated to the certificate authority for decrypting information received from the certificate authority via the certificate authority interface.

30. (Original) Electronic seal for a container, comprising

an interface accessible for entities participating in the transportation chain,

a log for recording data, and

a control unit for verifying data received via said interface, the control unit being designed for decrypting a digitally signed electronic container control certificate received via said interface, the decryption process using decrypt information stored in the log which decrypt information being associated to the transmitting entity.

31. (Original) Electronic seal according to claim 30, wherein the control unit is designed for storing the signed container control certificate in the log.

32. (Previously presented) Electronic seal according to claim 30, wherein the control unit is designed for considering the verification being failed if the signed container control certificate cannot be decrypted with the decrypt information stored in the log.

33. (Previously presented) Electronic seal according to claim 30,

wherein the control unit is designed for controlling a lock of the associated container, and

wherein a status of the container lock is subject to the result of the signature verification process.

34. (Previously presented) Electronic seal according to claim 30, wherein the control unit is designed for issuing a warning if the verification of the signature is considered to be failed.

35. (Previously presented) Electronic seal according to claim 30 wherein the control unit is designed for storing the container control certificate in the log if the verification succeeds.

36. (Previously presented) Electronic seal according to claim 30 wherein the decrypt information comprises a public key of the first entity in case a private--public key signing mechanism is used for signing the container control certificate at the transmitting entity.

37. (Previously presented) Electronic seal according to claim 30, comprising an interface for communicating with a location recording device associated to one of the entities, the control unit being designed for receiving location data from the location detection device via said interface.

38. (Original) Electronic seal according to claim 37, wherein the control unit is designed for storing the received location data in the log.

39. (Previously presented) Electronic seal according to claim 37, wherein the control unit is designed for verifying a digital signature of the received location data by a

corresponding function.

40. (Original) Electronic seal according to claim 39, wherein the control unit is designed for verifying the digital signature of the location data by applying decrypt information stored in the log and delivered to the log by a previous entity of the transportation chain.

41. (Previously presented) Electronic seal according to claim 39, wherein the control unit is designed for considering the verification to be failed if the signed location data cannot be decrypted with the decrypt information stored in the log.

42. (Previously presented) Electronic seal according to claim 39 wherein the control unit is designed for a storing the location data in the log subject to the result of the signature verification process.

43. (Previously presented) Electronic seal according to claim 30 wherein the control unit is designed for transmitting container identification information to a remote location recording device associated to one of the entities.

44. (Original) Electronic seal according to claim 43, wherein the control unit is designed for digitally signing the container identification information before the transmittal.

45. (Cancelled)

46. (Cancelled)

47. (Previously presented) System for documenting a transfer of authority of control for a container from a first entity of a transportation chain to a second entity of the transportation chain, the system comprising:

a computing unit according claim 27, which computing unit is associated to the first entity, and

an electronic seal comprising:

an interface accessible for entities participating in the transportation chain a log for recording data, and

a control unit for verifying data received via said interface, the control unit being designed for decrypting a digitally signed electronic container control certificate received via said interface, the decryption process using decrypt information stored in the log which decrypt information being associated to the transmitting entity which electronic seal is associated to the container.

48. (Previously presented) System for documenting transfer of authority of control for a cargo container from a first entity of a transportation chain to a last entity of the transportation chain, the transportation chain comprising one or more further participating entities, the system comprising:

a computing unit associated to the entities transferring authority of control, each of the computing units being designee according to claim 27, and

an electronic seal comprising:

an interface accessible for entities participating in the transportation chain a log for recording data,

and a control unit for verifying data received via said interface, the control unit being designed for decrypting a digitally signed electronic container control certificate received via said interface the decryption process using decrypt information stored in the log which decrypt information being associated to the transmitting entity which electronic seal is associated to the container.

49. (Previously presented) System according to claim 47, comprising a certificate authority for supporting the computing unit with cryptographic data as needed.

50 - 70. (Cancelled)